臺南市鹽水區公所個人資料風險評鑑程序書

發行單位：臺南市鹽水區公所
製訂單位：臺南市鹽水區公所
發行日期：2015 /11/23

修訂記錄				
修訂日期	版本	修訂編號	修訂頁次	修訂內容摘要
2015/11/23	V1.0			第一次發行

目　　錄

壹、 目的

臺南市鹽水區公所（以下簡稱本所)為依據「個人資料保護法」(以下簡稱本法)、「個人資料保護法施行細則」(以下簡稱細則)與相關法規規範，提供本所個資資產之相關單位，共同遵行之風險評鑑標準，以協助有效執行風險控管，預防個資外洩事件之威脅。

貳、 適用範圍

適用於本所各單位，本所所屬機關準用之。

參、 名詞定義(詳見個人資料保護法第二條)

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

十、威脅（Threat）：可能對系統或組織造成傷害之意外事件。

十一、弱點（Vulnerability）：因個資資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

十二、風險（Risk）：可能對團體或組織的資產發生損失或傷害的潛在威脅，通常用產生之影響及發生機率來衡量。

肆、 權責說明

一、本所各單位（以下簡稱各單位）應指定專人辦理下列事項：(詳見臺南市政府個人資料保護管理要點第三點)

(一) 當事人依本法第十條及第十一條第一項至第四項所定請求事項之考核。

(二) 本法第十一條第五項及第十二條所定通知事項之考核。

(三) 本法第十七條所定事項之公開或查閱。

(四) 本法第十八條所定個人資料檔案安全維護。

(五) 個人資料保護法令之諮詢。

(六) 個人資料保護事項之協調聯繫。

(七) 單位內個人資料損害預防及危機處理應變之通報。

(八) 本所個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。

(九) 其他單位內個人資料保護管理之規劃及執行。

二、本所應設置個人資料保護聯絡窗口，辦理下列事項： (詳見臺南市政府個人資料保護管理要點第四點)

(一) 公務機關間個人資料保護業務之協調聯繫及緊急應變通報。

(二) 重大個人資料外洩事件之民眾聯繫單一窗口。

(三) 各單位依前點指定專人之名冊製作及更新。

(四) 各單位依前點指定之專人與職員工教育訓練名單及紀錄之彙整。

伍、 程序說明

一、 為評估個人資料檔案之風險，本所應規劃個人資料風險評估與管理作

業，風險評估作業應包括下列項目：

（一）評估個人資料風險

1. 建立風險評量的標準(如下表所示)，包括：風險發生之機率與影響/衝擊之程度。個人資料檔案之風險評估應依據實際狀況，對照「影響及衝擊等級表」(如下表 1)及「風險發生可能性等級表」(如下表 2)之內容，並於「風險評鑑表」(參考附件 1)中進行之風險分析。

表 1：影響及衝擊等級表

評估項目	影響及衝擊等級表		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個資查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	可以間接識別特定當事人者	可以直接識別特定當事人者
個資數量	20筆以下 (團體訴訟不成立)	一般個資21~10,000筆 特種個資 21~1,000 筆	一般個資10,001筆以上 特種個資 1,001 筆以上
敏感程度	僅有一般識別資料，如姓名、服務單位、職稱、電子郵件地址等。	含有政府資料中之辨識者及財務資料等，如身分證統一編號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。	含有特種個人資料

表 2：風險發生可能性等級表

等級	評估標準
可能性低(1)	➢ 很少發生或無發生可能性。 ➢ 3 年期間沒有發生過。 ➢ 有相關控制措施，人員落實執行。

等級	評估標準
可能性中(2)	➢ 可能發生或偶爾發生。 ➢ 1 到 3 年期間發生次數小於 3 次。 ➢ 有相關控制措施但人員未落實執行。
可能性高(3)	➢ 經常發生。 ➢ 1 年內發生 2 次以上。 ➢ 無相關控制措施。

2. 各單位須針對各項個人資料之使用及控管狀況，依據「影響及衝擊等級表」之各個評估項目，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「風險評鑑表」。
3. 識別風險發生之可能性及影響/衝擊程度，將此 2 項評分進行相乘，即求出該個人資料檔案之風險值。風險值=風險發生可能性等級x影響及衝擊等級表。
4. 將經由風險值計算公式所得之風險值，對應至「風險分布矩陣圖」(如下圖 1)以判斷風險值之分布情況。

圖 1：風險分布矩陣圖

風險分布矩陣			
	風險發生可能性		
影響及衝擊等級表	可能性低(1)	可能性中(2)	可能性高(3)
非常嚴重(3)	中(3)	高(6)	高(9)
嚴重(2)	低(2)	中(4)	高(6)
輕微(1)	低(1)	低(2)	中(3)

（二）處理個人資料風險

依風險評估結果，對於風險值為 6 或 9 之個人資料檔案進行風險處理，擬定改善措施，並填入「風險評鑑表」。

二、 覆核

（一）持續改善

為保持本風險評鑑方法之有效性與適用性，本所各單位應定期檢討「風險評鑑表」之項目，以期確保本所個資資產均處於最佳保護之下。

（二）風險重新評估

1. 每年應至少執行 1 次風險評鑑。
2. 當範圍內有以下的狀況發生之時，則實施不定期的複核，以更新及確保個資資產風險評估的正確性及完整性：
   (1) 有新增、變更或移除個資資產。
   (2) 組織業務調整。
   (3) 個資外洩發生。

陸、 相關文件

無。

柒、 附件

附件 1：風險評鑑表(樣本)

單位名稱	
單位主管	
評鑑人員	

個人資料檔案名稱	影響及衝擊				可能性	風險值	風險等級	改善措施(如風險等級為高時)
	可識別性	個資數量	敏感程度	評估項目最大值(即為影響及衝擊等級)				